Security verification for continuous variable quantum key distribution

Yi-Bo Zhao, Zheng-Fu Han,* and Guang-Can Guo

Key Lab of Quantum Information, University of Science and Technology of China, (CAS), Hefei, Anhui 230026, China

Noise estimate is crucial to the continuous variable quantum key distribution. In the estimate many parameters should be evaluated, including the mean, variance, attenuation and the normality. Then how the inaccuracies of so many parameters affect the security becomes a problem. Here we will discuss a test method and illustrate the relationship between its inaccuracy and the amount of secret keys. Through analyzing Eve's possible attack way of obtaining additional information, we show which parameter is determinant under specific conditions. Finally, we will see that the minimum sample size for the channel test should be exponentially proportional to the transmission distance.

PACS numbers: 03.67.Dd, 42.50.-p, 89.70.+c

I. INTRODUCTION

Quantum key distribution (QKD) is of great importance to the cryptograph. Up to now there are two main kinds of schemes, single photon [1] and continuous variable (CV) [2, 3, 4, 5, 6, 7] one. Compared with the single photon one, the CVQKD does not require the single photon detector and source and thus is expected to provide high secret key rate. At present, there are several schemes that have been suggested for the CVQKD, including the direct reconciliation (DR) [14], reverse reconciliation (RR) [2, 4, 5, 6], DR&post-selection (PS) [3, 7] and RR&PS [8, 9] one. Among these schemes, the DR one cannot break the 3dB loss condition. To break the 3dB limit, the RR or PS should be employed. The DR&PS has a good performance on resisting the excess noise, but its secret key rate decreases sharply with the increase of the channel loss. The RR scheme is presented by Grosshans *et al* and supposed to be potential to provide high secret key rate over arbitrary distance. However, In Ref. [15], Zhao *et al* showed that a secret key cannot be distilled for the Gaussian modulated pure RR scheme at too long transmission distance just for the imperfection of practical error corrections. To make the RR scheme feasible the PS should be introduced. In Ref. [8, 9, 10], Heid and Zhao *et al* respectively showed a way to combine the RR scheme with the PS. Zhao *et al* demonstrated that if the PS and other tactics are utilized for the CVQKD, secret keys can be distilled with high efficiency over 100 km fiber by practical error corrections [10]. Heid and Lütkenhaus proved that the PS also can make the RR scheme resist more excess noise [9]. Moreover, many of recent experiments showed the feasibility of the CVQKD [6, 11, 12, 13]. In Ref. [13], Lance *et al* established the secret keys rate 1k/s for 90% channel loss, which is really high compared with the single photon one [21]. Therefore, it is expected that the CVQKD plays an important role for the cryptography in the future.

For the RR, DR&PS and RR&PS schemes, the conditional noise estimate is crucial. In Refs. [2, 10], it has been showed that if the conditional noise and entropy estimate is employed, various channel noises introduced by Eve can be restrained, so that the security of arbitrarily modulated scheme and the reconciliation can be guaranteed. Also in Refs. [8, 9], it is assumed that the noise between Alice and Bob is Gaussian. Then the accurate estimate of the conditional noise distribution is important for the CVQKD. It is known that an unknown parameter cannot be estimated by the statistical method without any error, nevertheless, the security of the CVQKD is much sensitive with parameter inaccuracies [2, 6], and a small estimate error may cause the security analysis totally wrong. Moreover, the number of the parameters of a totally unknown distribution is infinite in principle, whereas the estimable statistics is finite. Then how to test the channel effectively and how much errors can be tolerated should be given.

Here, we introduce the hypothesis testing to check the channel, which is going to be discussed mainly for schemes suggested in Refs. [2, 10], but also effective for other kinds of CVQKD. We assume the channel secure at first and then test whether this assumption is true, so that a judgment criterion can be given. For the statistical fluctuation, the estimated parameter of an insecure system may show it secure topsy-turvy. In the following it can be seen that through the hypothesis test this problem can be solved, but certain amount of secret keys should be given up to compensate this fluctuation. Consequently, we show that to obtain a high confidence and low secret key loss at the same time, the minimum sample size should be exponentially proportional to the length of the transmission line. To illustrate the influence of the estimate inaccuracy to the security, in the following, we will discuss Eve's possible attack in detail. Finally it can be seen that this test can restrain Eve's attack effectively and the conditional variance estimate is enough to limit Eve's eavesdropping while the bit assignment efficiency is always 100%, whereas the normality test is crucial if this efficiency is low.

*Electronic address: zfhan@ustc.edu.cn

II. CHANNEL TEST

In the CVQKD protocol presented in Ref. [2] Alice sends a random coherent state $|a\rangle$ to Bob. Then Bob measures its x or p quadrature through the homodyne detection. If all the apparatus are ideal then Bob's measurement result will obey a Gaussian distribution of mean $\sqrt{G}\alpha_x$ ($\sqrt{G}\alpha_p$) and variance N_0, where G denotes the channel transmission efficiency and N_0 denotes the variance of vacuum noise [2, 4]. However, in practice the apparatus noise and Eve's attack are inevitable, so the distribution of Bob's measurement results may deviate from the above Gaussian noise distribution. It has been shown that if this distribution can be maintained to be Gaussian and of mean $\sqrt{G}\alpha_x$ ($\sqrt{G}\alpha_p$) as well as variance $N_0+\delta N_0$, the security of CVQKD can be guaranteed, where δN_0 should be smaller than $\gamma G N_0$ and γ is a parameter determined by Alice's modulation [2] and the reconciliation [10]. Generally speaking, the small noise introduced by apparatus is always Gaussian. Then if without Eve's attack, this condition can be satisfied. While under Eve's attack, if this distribution is changed to the non-Gaussian or the δN_0 is increased larger than $\gamma G N_0$, Alice and Bob will cancel this communication. Then Eve cannot steal any useful information in the effective communications. Now a problem posted to Alice and Bob is how to estimate the conditional distribution.

Suppose after many quantum communications, Alice and Bob publish their continuous variables $A_x = \{a_{x,1}, a_{x,2}, \ldots, a_{x,n}\}$, $A_p = \{a_{p,1}, a_{p,2}, \ldots, a_{p,n}\}$, $B_x = \{b_{x,1}, b_{x,2}, \ldots, b_{x,n}\}$ and $B_p = \{b_{p,1}, b_{p,2}, \ldots, b_{p,n}\}$ to estimate the channel, where the index x and p denote the variable measured from x and p quadratures. Since the x and p quadratures are always symmetric, in the following, we will no longer distinguish them and simply employ a and b to describe Alice and Bob's variables respectively. If there is no eavesdropping, the distribution of their data will be of the Gaussian noise case, satisfying

$$P(b_i|a_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp[-\frac{(\sqrt{G}a_i - b_i)^2}{2\sigma^2}], \qquad (1)$$

where the σ^2 denotes the variance of the noise between Alice and Bob and G is the channel transmission [3]. In the practical system the σ^2 is always unknown and needs to be estimated. Theoretically, the variance satisfies $\sigma^2 \geq N_0$. One necessary condition of the security is $\sigma^2 \leq N_0 + \gamma G N_0$ [2]. During the communication, there may be Eve's attack and channel noise, so that the noise may no longer be Gaussian and the σ^2 may be larger than $N_0 + \gamma G N_0$. Then Alice and Bob should utilize those data to detect the eavesdropping. If finding that the noise is not the additive Gaussian of variance less than $N_0 + \gamma G N_0$ as well as mean zero, they will judge this system insecure and give up all the data. While testing the channel, Alice and Bob should guarantee that if the channel is insecure they find it at least with probability $1-\beta$, where β is an exponentially small positive number, and if the channel is secure they should judge it secure with a high probability. Define the hypotheses H_0: the channel is secure, and H_1: the channel is insecure. Also define the type I error as the case that Alice and Bob reject the hypotheses H_0 while the channel is secure, and the type II error as that they accept the hypotheses H_0 while the channel is insecure. Then in the QKD we require that the probability of happening type II error is exponentially small and that of happening type I error is not too large.

In practice, we should estimate σ^2 with high confidence coefficient within the interval $[N_0, N_0 + \gamma G N_0)$, where G may be of order $O(0.1)$, and consequently the required sample size is very large. Therefore the test method should be with high performance and low computational complexity while $n \to \infty$.

There are many normality test methods now, including the chi-square goodness of fit test, called χ^2 test in the following, Kolmogorov-Smirnov, W, D, kurtosis and skewness test [16, 17, 18, 19], where W and D test are difficult to deal with the large sample, Kolmogorov-Smirnov test requires the tested distribution is known. The kurtosis and skewness tests have a better performance than the χ^2 test under certain condition but are insufficient to test the normality. Therefore we employ the χ^2, kurtosis and skewness tests to do the normality test in the following. The channel noise test can be implemented by the following steps.

1. Test the hypotheses, H_0^1: $\mu = 0$, H_1^1: $\mu \neq 0$, where μ describes the mean value.

2. If the H_0^1 is accepted, test the hypotheses, H_0^2: $\sigma^2 < N_0 + \gamma G N_0$, H_1^2: $\sigma^2 \geq N_0 + \gamma G N_0$.

3. If the H_0^2 is accepted, test the hypotheses, H_0^3: $\beta_s = 0$, H_1^3: $\beta_s \neq 0$, where β_s denotes the skewness.

4. If the H_0^3 is accepted, test the hypotheses, H_0^4: $\beta_k = 3$, H_1^4: $\beta_k \neq 3$, where β_k denotes the kurtosis.

5. If H_0^4 is accepted, test the hypotheses, H_0^5: the noise is Gaussian, H_1^5: the noise is non-Gaussian.

If H_0^5 is accepted, then Alice and Bob can be sure about that the channel is secure. Here we require that the type I error and the type II error probabilities are smaller than α and β respectively. In the above tests, the H_1 hypotheses of 1, 3, 4, 5 steps are irrational, since we can always accept them. To solve this problem, we will introduce the estimate error in the following. If the errors belong to certain range, we reject the H_1 hypotheses. Later we will discuss influences of this inaccuracy to the security.

We estimate the mean value μ through $\overline{(\sqrt{G}a - b)}$. For convenience, set $X = (\sqrt{G}a - b)$, which will be called noise in the following. The test Φ_1 defined as that if

$\left|\bar{X}\right| \leq C_1$, accept H_0^1, else reject it. The σ can be estimated through S, where $S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \bar{X})^2$. Then $\sqrt{n}(\bar{X}-\mu)/S$ obeys the student distribution of freedom n-1, which will be simply called t distribution in the following. The density function of the t distribution of freedom n is given by $t_n(y) = \Gamma[(n+1)/2]/[\sqrt{n\pi}\Gamma(n/2)](1+y^2/n)^{-(n+1)/2}$, where Γ is the Gamma function given by $\Gamma(n/2) = 1\cdot 3\cdot 5\cdots(n-2)\cdot 2^{-(n-1)/2}\sqrt{\pi}$. In the following, we use $t_{n-1,\alpha}$ to denote the α quantile of the t distribution, defined by $\int_{-\infty}^{t_{n-1,\alpha}} t_{n-1}(y)dy = 1-\alpha$. Then the test Φ_1 becomes that while $\left|\sqrt{n}\bar{X}/S\right| < t_{n-1,\alpha/2}$, accept H_0^1. We see that if the H_0^1 is accepted, the μ belongs to the region $(-St_{n-1,\alpha/2}/\sqrt{n} - St_{n-1,\beta/2}/\sqrt{n}, St_{n-1,\alpha/2}/\sqrt{n} + St_{n-1,\beta/2}/\sqrt{n})$ with confidence coefficient β.

Under some condition, the line transmission ratio G may be also unknown and require the estimate. The G can be estimated through the maximum likelihood method. According to Eq. (1), define the likelihood function

$$L = \sum_{i=1}^{n}\log P(b_i|a_i) = -\frac{n}{2}[\log(2\pi\sigma^2)] - \frac{1}{2\sigma^2}\sum_{i=1}^{n}(\sqrt{G}a_i - b_i)^2.$$

Then $\partial L/\partial\sqrt{G} = 0$ shows that we can use $\sum_{i=1}^{n} a_i b_i / \sum_{i=1}^{n} a_i^2$ to estimate $\sqrt{G}$.

In the step 2 we can use $S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \bar{X})^2$ to estimate σ^2. It is known that the $(n-1)S^2/\sigma^2$ obeys the chi-square distribution of freedom $n-1$ (denoted by χ^2_{n-1} in the following) [26]. Define the α quantile $\chi^2_{n-1,\alpha}$ of the χ^2_{n-1} distribution by $\int_{-\infty}^{\chi^2_{n-1,\alpha}}\chi^2_{n-1}(y)dy = 1-\alpha$. Then the test Φ_2 of the step 2 becomes that if $(n-1)S^2 < (N_0 + \gamma G N_0)\chi^2_{n-1,\alpha}$ accept H_0^2. To reduce the type II error probability below β Alice and Bob should accepte H_1^2 while $(n-1)S^2 > (N_0+\gamma G N_0)\chi^2_{n-1,1-\beta}$. Here we see that α and β cannot be both small at the same time. Actually, a reasonable hypotheses H_0^2 should be $\sigma^2 < \sigma_0^2$, where the σ_0^2 denote the variance of practical system noise. Then the test Φ_2 becomes accepting H_0^2 while $(n-1)S^2 < \sigma_0^2\chi^2_{n-1,\alpha}$. While $(1+\gamma G)N_0 > \sigma_0^2 \geq N_0$, we have

$$(1+\delta)\chi^2_{n-1,\alpha} < (1+\gamma G)\chi^2_{n-1,1-\beta}, \quad (2)$$

where $\delta = (\sigma_0^2 - N_0)/N_0$. It can be seen that to obtain a low α and β at the same time, we should set the sample size large enough.

In the step 3, we introduce the statistical quantity $\tau_s = \frac{\sqrt{n}\sum(X_i-\bar{X})^3}{[\sum(X_i-\bar{X})^2]^{3/2}}$. The test Φ_3 of step 3 can be defined as that if $|\tau_s| < C_3$, accept H_0^3. Under the condition that the distribution is normal, the first and second moments of the distribution of τ_s respectively are [20]: $E(\tau_s) = 0$, $D(\tau_s) = \frac{6(n-2)}{(n+1)(n+3)}$. Then according to the Chebyshev inequality, we have $P(|\tau_s| > \alpha) \leq D(\tau_s)/\alpha^2$. Then in the skewness test $C_3 \leq D(\tau_s)/\alpha^2$.

In the step 4, we introduce the statistical quantity $\tau_k = \frac{n\sum(X_i-\bar{X})^4}{[\sum(X_i-\bar{X})^2]^2}$. The test Φ_4 of step 4 can be defined as accepting H_0^4 if $|\tau_k - 3| < C_4$. While the distribution is normal, the first and second moments of the distribution of τ_k respectively are [20]: $E(\tau_k) = \frac{3(n-1)}{n+1}$, $D(\tau_k) = \frac{24(n-2)(n-3)}{(n+1)^2(n+3)(n+5)}$. Therefore, in the kurtosis test $C_4 \leq D(\tau_k)/\alpha^2$.

Here we employ the χ^2 test to check the normality. Set $K = 20$. At first we divide the interval $(-\infty,\infty)$ into K parts, $I_1 = (k_0, k_1]$, $I_2 = (k_1, k_2]$, $\ldots$, $I_K = (k_{K-1}, k_K)$, where $k_i = (N_{i/K} - \bar{X})\sigma$ and $N_{i/K}$ is the $1-i/K$ quantile of the standard normal distribution. It can be seen that the whole interval is divided with equiprobability. Define the statistical quantity $Z = \sum_{i=1}^{K} K(n_i - n/K)^2/n$, where n_i describe the number of samples that belong to the interval I_i. Since there are three unknown parameters, It can be seen that Z obeys the χ^2 distribution of freedom $K-4$ [17]. Then the test of H_0^5 becomes Φ_5: accept H_0^5 while $Z < \chi^2_{K-4,\alpha}$. Because in the χ^2 test we divide the whole interval into several small intervals and actually only check the distribution of the small intervals, we cannot test the distribution within each small interval. In practice, we can suppose that the fine distribution within the small intervals cannot be controlled by Eve and thus is needless to be checked.

We can see that $Z = \sum_{i=1}^{K} n(f_i - P_i)^2/P_i$, where P_i describes the assumed probability of the interval I_i and f_i describes the practical frequency that the samples belong to I_i. While reducing the probability of type I error, we should also exponentially lower the probability of type II error. If under the condition that the theoretical distribution is unknown, Alice and Bob can use f_i to estimate P_i. However, the distribution of Z obeys the χ^2 distribution at $n\to\infty$ only when the H_0^5 is valid. Here we can do an approximation, still regarding the distribution of Z as χ^2 while P_i slightly deviate from the assumed value. If we estimate the P_i by f_i, the confidence interval of P_i with confidence coefficient $1-\beta$ is $f_i \pm \delta P_i$. Then we approximately have $Z = \sum_{i=1}^{K} n\delta P_i^2/P_i$ obeying the χ^2 distribution. Therefore the δP_i satisfies $\sum_{i=1}^{K} n\delta P_i^2/P_i < \chi^2_{K-4,\beta}$ and $\sum\delta P_i = 0$. While the H_0^5 is valid, the practical f_i may also deviate from the normality distribution with δf_i, where δf_i satisfies $\sum_{i=1}^{K} n\delta f_i^2/P_i < \chi^2_{K-4,\alpha}$ and $\sum\delta f_i = 0$. Then we can see that if the real distribution deviates from the normal with $|\delta P_i + \delta f_i|$, we may also accept the H_0^5 hypothesis.

III. TEST DISCUSSION

In the above we discussed how to do the normality test. Here we will analyze its inaccuracy. Because of the instability and Eve's attack, the above tested parameters are

not always constants [21]. Then Alice and Bob should test them not only for the eavesdropping detection but also for many other processes, such as reconciliation [10] and system adjustment. Therefore, we should not only discuss the misjudgment probability but also show the influence of the estimate inaccuracy to the following processes. Moreover, it is possible that Alice and Bob cannot distinguish whether the noise is caused by the environment or Eve's disturbance. In the security analysis, a rational assumption is that all the noise is introduced by Eve's attack. Since the environment noise is inevitable, Alice and Bob do not abort the communication while detecting the eavesdropping or the excess noise but cancel it while parameters exceed certain threshold. Thus, although in the above test we assume that the mean of the noise is zero and the distribution of it is normal, we do not give up these communications while their real value slightly departure from the assumed one. In practice, even if we accept the above hypotheses, we may still evaluate the parameters by the estimated results rather than the assumed value. Here, we employ the hypothesis test to check the channel, because the estimated value does not always represent the real one and the statistical errors are ineluctable. Then even though a system is insecure at all, the estimated value may show it secure. Thus we should have some preconception about the system, assuming it secure or insecure beforehand and only when the result show the hypothesis obviously wrong, will we reject it.

While we do the sampling check, the exposed variable should be discarded. Then the test results are only useful for the remained un-sampled variables, so they should represent the parameters of the remained variables accurately.

It is possible that the mean of the noise is non-zero, for example, while the zero point of apparatus has not been corrected. The inaccuracy of the estimate of the mean will affect Alice and Bob's following coding. For example, while $\mu = 0$, coding b_i larger than zero to binary digit 1 and b_i smaller than zero to 0 is a symmetric assignment to Alice and Bob. If $\mu \neq 0$ and they do not know it, the coding will no longer be symmetric. In principle, only the mean deviating from zero does not allow Eve to obtain more of Bob's information, but in practice it will lower Alice and Bob's reconciliation efficiency and thus affect the security [10]. The inaccuracy of the mean estimate is equivalent to adding a noise to Alice and Bob's coding. The maximum variance of this noise is smaller than $(\bar{X}-\mu)^2$. While the H_0^1 is accepted, $(\bar{X}-\mu)^2 \leq S^2(t_{n-1,\alpha/2}+St_{n-1,\beta/2})^2/n$. The information loss caused by this inaccuracy becomes

$$\delta I_u \leq \frac{1}{2\ln 2}\frac{S^2(t_{n-1,\alpha/2}+t_{n-1,\beta/2})^2}{nN_0} \tag{3}$$

with probability at least $1-\beta$, where we have done an approximation to the Shannon information [23]. This loss should not exceed the amount of secret keys. Then we have

$$S^2(t_{n-1,\alpha/2}+t_{n-1,\beta/2})^2 \leq n\gamma G N_0 \tag{4}$$

Actually, for a system that has been strictly zero adjusted, we may believe the mean is zero, while the estimated value is slightly deviate from it.

The variance of the noise can affect the mutual information between them and the amount of Eve's attacked additional information [2]. To guarantee the security, we require the probability of type II error smaller than β. While the hypotheses H_1^2 is rejected, we should not regard S^2 as the real variance, but determine it by the confidence interval. If the estimated variance is S^2 then the real variance is smaller than $(n-1)S^2/\chi^2_{n-1,1-\beta}$ with probability larger than $1-\beta$. Then we should regard $(n-1)S^2/\chi^2_{n-1,1-\beta}$ as the real variance for the confidence, although the variance of the noise introduced by Eve is S^2 with high probability. The variance of the equivalent noise introduced by the inaccuracy of the estimate is $[(n-1)/\chi^2_{n-1,1-\beta}-1]S^2$. It can be seen that to ensure the system secure with high probability, certain amount of secret keys should be sacrificed.

The accuracy of the normality test will influence entropies. The conditional entropy between Alice and Bob can be defined as $H(B|A) = -\sum_{i=1}^{K} P_i \log_2 P_i - \Delta$, where Δ is a constant determined by K [23]. If H_0^5 is valid, we have $P_i = 1/K$ and $H(B|A) = \log_2 K - \Delta$. While the P_i is perturbed, $P_i \to P_i + \delta P_i'$, the entropy will be changed by $\delta H(B|A) = -\sum_{i=1}^{K}\delta P_i' \log_2 P_i - \sum_{i=1}^{K}\delta P_i' - \sum_{i=1}^{K}\delta P_i'^2/P_i = -\sum_{i=1}^{K}\delta P_i'^2/P_i$. The maximum perturbation can be given by $|\delta P_i + \delta f_i|$. Then we have

$$\delta H(B|A) \leq 2(\chi^2_{K-4,\alpha}+\chi^2_{K-4,\beta})/n. \tag{5}$$

IV. SECURITY ANALYSIS

A. Eve's attack, in general

It has been shown in Refs. [2, 10] that to obtain Bob's information, Eve has two direct information sources, Alice and Bob. Then she can utilize the information received from these two sources to estimate Bob's variables. The maximum information Eve can obtain from Alice is restricted by the Holevo bound [2]. While using this information to estimate Bob's keys, Eve should estimate the channel between Alice and Bob well at first. Then she can estimate Bob's key through a Markovian channel *Eve* $\to$ *Alice* $\to$ *Bob*. If there is no excess noise, the noise on Bob's side is the minimum vacuum noise and there is no opportunity left to Eve to control the noise [2]. However, the excess noise is inevitable in practice. Under the condition of excess noise, Eve can control the fine noise distribution to obtain a better estimate, but she should guarantee the total average noise distribution can pass the channel test. Then her ability of controlling Alice and Bob's channel is limited. Eve may control

Bob's channel through various methods, one example of which is the entangling cloner [6] presented by Grosshans *et al*. Here we do not care about Eve's concrete attack while just discuss all possible fine noise distributions that may allow Eve to learn additional information. If Eve does not control Alice and Bob's channel noise, she can learn certain amount of information from Bob through the Markov chain. While utilizing the channel noise, her obtained information will be more than that obtained purely through the Markov chain. The additional information obtained through utilizing the channel noise can be regarded as obtained through the non-Markovian way, and will be called non-Markovian information in the following.

Here, we will discuss the possible eavesdropping under the tests Φ_1 to Φ_5. The samples of these tests are randomly sampled from a large number of variables. Only when distributions of remained un-sampled variables are independent and identical with that of the samples, the estimated distribution is that of the remained variables. Actually, the independence and identicalness are not always true. Eve can attack each variable through different method, and then the identicalness can be broken. There may be such case that some variables are totally attacked but not sampled by the estimation. Then it will leave Eve more opportunity to obtain the secret keys. In the CVQKD, we allow Eve to obtain certain amounts of information, whereas if she cannot steal all the information, we can always establish the pure secret keys through the privacy amplification [24]. Then Alice and Bob can just test whether Eve has attacked the whole information. Here we can suppose that Eve's attack is effective only when she employ it to steal a considerable deal of keys that occupy certain proportion in the whole variables. Since each communication will be sampled by the same probability and Eve cannot know which variable will be sampled, for her each key is identical. Then any of Eve's effective attack method cannot escape from the sampling. Suppose Eve's attack E will cause the noise between Alice and Bob to be $P_E(X|a,e)$, where e denotes Eve's possible state. This attack will be sampled with the probability $\Pr(sampling|a,E) = \Pr(sampling)$. Suppose Eve employs the tactic E with probability $P(E|a)$ in attacking m samples ($m \to \infty$), where it has been assumed that Eve's decision depends on Alice's variables. Then Alice and Bob's sampling test is to check the distribution

$$\begin{aligned} P_0(X) &= \coprod_e [\sum_{a,E} P_E(X|a,e)\Pr(sampling|a,E) \\ &\quad \times P(a,E)/\Pr(sampling)] \\ &= \coprod_{a,e} [\sum_E P_E(X|a,e)P(E|a)], \end{aligned} \tag{6}$$

where $\coprod_x \rho$ denotes $\sum_x [\rho \Pr(x)]$. Of course that $P_0(X)$ passes the tests Φ_1 to Φ_5 dose not mean that each $P_E(X|a,e)$ can pass.

In the reverser reconciliation CVQKD, to attack Bob's information Eve has two channels to employ, a Markovian and a non-Markovian channel [2]. The channel noise allows Eve to obtain non-Markovian information. Here we will call all the attack that utilizes the channel noise non-Markov attack. Eve's attack should guarantee that noise between Alice and Bob can pass the tests Φ_1 to Φ_5. Then the non-Markovian information obtained through non-Markov attacks is given by $I(E:B|A,\Phi_1,\ldots,\Phi_5)$. Here, we will discuss this information in detail and give Eve's possible attacks under the channel test.

B. Eve's attack, neglecting the reconciliation

In Eq. (6), we can see that even though the variance of $P_0(X)$ can pass the test Φ_2, the variance of some $P_E(X|a,e)$ may be far from hypothesized variance. Suppose Eve's attack E_{σ^2} will cause the noise between Alice and Bob to be $P(X|a,E_{\sigma^2}) = \coprod_e P_{E_{\sigma^2}}(X|a,e)$ of variance σ^2, where we have already supposed that Eve's attack is symmetric to quadratures x and p. It has been shown that $H(B_x|E,A_x) + H(B_p|E,A_p) \geq 2H_0$ [2, 4, 25]. Then the maximum information that can be obtained through the non-Markovian channel becomes $\max H(B|A) - \min H(B|E,A) = 2[\max H(B|A) - H_0]$. Set $H'_{\sigma^2} = 0.5\log_2 \frac{\sigma^2}{N_0}$, which is the maximum entropy while the variance is σ^2. It can be seen that the maximum non-Markovian information under the attack E_{σ^2} is $2H'_{\sigma^2}$.

If Eve randomly chooses method $E_{\sigma_i^2}$ with probability $P_{\sigma_i^2}$ to attack, then to pass the Φ_2 test she should maintain $\sum P_{\sigma_i^2}\sigma_i^2 \leq \sigma_0^2$. Here, we can see that besides obtaining the information through each attack $E_{\sigma_i^2}$ Eve can also learn the information from the variation of σ_i^2, which means that random changing the $E_{\sigma_i^2}$ can also establish certain amount of information between her and Bob. This information cannot be known by Alice, since she does not know which $E_{\sigma_i^2}$ is chosen by Eve. The amount of the information carried by the variation of σ_i^2 can be evaluated by the following way. If without this information, the entropy of Bob's noise is $\Theta[\coprod_a \sum P_{\sigma_i^2} P(X|a,E_{\sigma^2})]$, where $\Theta(\rho)$ denotes the Shannon entropy of the probability density function ρ [23]. If this information is known, then the average conditional entropy of Bob's measurement is $\coprod_a \sum P_{\sigma_i^2}\Theta[P(X|a,E_{\sigma^2})]$. Therefore, the information carried by the variation of σ_i^2 is $\Theta[\coprod_a \sum P_{\sigma_i^2} P(X|a,E_{\sigma^2})] - \coprod_a \sum P_{\sigma_i^2}\Theta[P(X|a,E_{\sigma^2})]$. If Eve randomly changes the $E_{\sigma_i^2}$ and maintain each $P(X|a,E_{\sigma^2})$ to be Gaussian, the $P_0(X)$ may become non-Gaussian, whose entropy is smaller than that of the Gaussian one if under the same variance condition. Finally, Eve's maximum attacked information through the

non-Markov channel is

$$\begin{aligned} & 2\sum P_{\sigma_i^2} H'_{\sigma_i^2} + \Theta[\coprod_a \sum P_{\sigma_i^2} P(X|a, E_{\sigma^2})] \\ & - \coprod_a \sum P_{\sigma_i^2} \Theta[P(X|a, E_{\sigma^2})] \\ \leq & \sum P_{\sigma_i^2} H'_{\sigma_i^2} + H'_{\sigma_0^2}. \end{aligned}$$

Since $\sum P_{\sigma_i^2} H'_{\sigma_i^2} \leq H'_{\sigma_0^2}$ and the equal is satisfied only when $\sigma_i^2 = \sigma_0^2$, Eve's optimal attack is to attack all the variables through $E_{\sigma_0^2}$.

Eve can steal Bob's information through obtaining a better estimate of Alice and Bob's channel. For the Markovian channel $Eve \rightarrow Alice \rightarrow Bob$, if the mutual information between Alice and Bob is increased, that between Eve and Bob may be also increased. Then Eve can control Alice and Bob's channel and randomly optimize it. If this optimization regularity is not known by Alice and Bob, they cannot obtain more information through this optimization but Eve can. To optimize Alice and Bob's channel, Eve should control the channel noise. Suppose Eve's attack E_ρ can make the noise between Alice and Bob to be $\rho(X|a, e)$. While Eve employs a set of $E = \{E_{\rho_i}, \Pr(E_{\rho_i})\}$ to attack, where $\Pr(E_{\rho_i})$ denotes the probability of the method E_{ρ_i}, the total noise introduce on Bob's side becomes $\rho_0 = \sum_{E_{\rho_i}} \Pr(E_{\rho_i})\rho_i$. Alice and Bob can only know the $\coprod_{a,e} \rho_0$ through the channel test but cannot know the exact ρ_i, which is known by Eve. If the channel noise were ρ_i, the mutual information between Alice and Bob will be larger than that under the ρ_0 noise condition, which means that if knew the exact variables of Alice, Eve could estimate Bob's variables more precisely than Alice. Then after learning Alice's information, she can estimate Bob's quadratures through the optimized Markov chain better than she estimate it with ignorance of ρ_i and thus obtain some additional information. The amount of this additional information is determined by the variation of ρ_i. As previous analysis, the information carried by the variation of ρ_i is $\Theta(\coprod_{a,e} \rho_0) - \coprod_{a,e} \sum \Pr(E_{\rho_i})\Theta(\rho_i)$. If Eve brings a noise ρ_i to one of Bob's quadrature, she certainly brings a conjugate noise $\bar{\rho}_i$ on the other quadrature. With the large enough sample size, both ρ_i and $\bar{\rho}_i$ will be sampled by Alice and Bob with equiprobability. For the uncertainty theorem, we have $\Theta(\rho_i)+\Theta(\bar{\rho}_i) \geq 2H_0$ [2, 4, 25]. The noises on two conjugate quadratures are not always symmetric. Alice and Bob is to estimate the noises on both quadratures separately, so although ρ_i and $\bar{\rho}_i$ are sampled with the same probability in total, Eve can control their sampled proportion in one quadrature estimation. Suppose, while Alice and Bob estimate the x quadrature, the ρ_i and $\bar{\rho}_i$ are respectively occupy the proportion of $\Pr(E_{\rho_i})P_x$ and $\Pr(E_{\rho_i})(1-P_x)$. Then while they estimate the p quadrature, they will occupy the proportion of $\Pr(E_{\rho_i})(1 - P_x)$ and $\Pr(E_{\rho_i})P_x$ respectively. The $\sum \Pr(E_{\rho_i})\Theta(\rho_i)$ actually becomes $\sum \Pr(E_{\rho_i})[P_x\Theta(\rho_i) + (1 - P_x)\Theta(\bar{\rho}_i)]$. Eve should guarantee that noises on both quadratures can pass the channel test. Then the minimum $\sum \Pr(E_{\rho_i})[P_x\Theta(\rho_i) + (1 - P_x)\Theta(\bar{\rho}_i)]$ is given by $H_0 - H'_{\sigma_0^2}$. Since $\Theta(\coprod_{a,e} \rho_0) \leq H_0 + H'_{\sigma_0^2}$, the maximum information Eve can attack through this way is still $2H'_{\sigma_0^2}$.

In the above discussions we can see that no matter how Eve attacks Bob's information, the maximum non-Markovian information she can obtain from the non-Markov channel is $2H'_{\sigma_0^2}$. Also no matter what Alice's modulation is, only when the noise between Alice and Bob is Gaussian, can the amount of Eve's non-Markovian information approach the maximum. Alice and Bob can limit Eve's obtained information just through the variance test, and the normality test is unnecessary.

C. Eve's attack, utilizing the reconciliation

To establish the final binary secret keys mapping those continuous variables into common binary bit is required [10, 22], so while considering the security of CVQKD, we should also take the reconciliation into account [10]. The reconciliation is always constituted by quantization, the coding and the error correction. Here we only consider the quantization and the coding (QC). After the QC, the mutual information between Alice and Bob becomes $\xi I(A : B)$, where ξ is the efficiency of QC. The efficiency of the QC will depend on the type of the channel noise. Under this condition, while the noise is changed, not only $I(A : B)$ and $I(E : B)$ will be changed, but also ξ will be alternated. Then Eve can control both $I(A : B)$ and the ξ to attack more information. The influence of the noise to the QC efficiency can be illustrated by the figure 1, where the solid and doted line respectively describe distributions of the variables under two kinds of noises. The coding method is to code the $x < 0$ to 0 and $x \geq 0$ to 1. We can see that if under the condition of the noise denoted by the solid line, the QC efficiency is lower than 100%, while if under the condition of the noise denoted by the doted line, the efficiency is 100%, since before and after the QC the mutual information remained to be 1 bit.

Because the ξ is not a constant, $I(E : B) < I(A : B)$ no longer means the CVQKD secure after the QC. For the QC presented in Ref. [10], it has been shown that if we introduce the noise estimate into the reconciliation, Eve's attack is largely limited to the Markovian attack and the non-Markovian attack is still determined by the excess noise.

If Eve takes no account of the QC, her information attacked through the non-Markov channel will be smaller than $2H'_{\sigma_0^2}$-bit, large portion of which may be lost during the QC. To steal as much information as possible Eve should adjust the noise to reduce the loss of the non-Markovian information, while the average introduced noise should pass the channel test. Suppose ξ_ρ is the QC efficiency and $I_\rho(A : B)$ is the mutual information be-

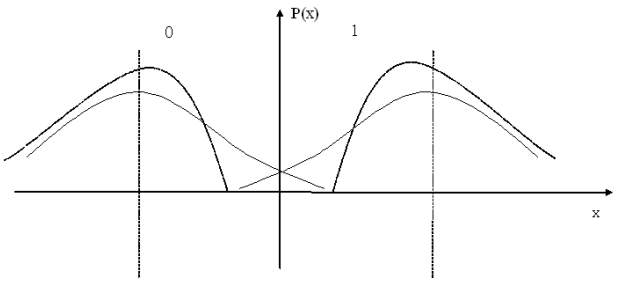

FIG. 1: Illustration of the influence of the noise to the quantization and coding efficiency, where the solid and doted line respectively denotes the case of two kinds of noise. It can be seen that the noise denoted by the doted line has no influence to the quantization.

tween Alice and Bob while the channel noise is $\rho(X|a,e)$. If there is Eve's attack, Alice and Bob cannot know the exact $\rho(X|a,e)$ in each communication. They can only know the average noise estimated by the channel test. However, Eve can utilize $\rho(X|a,e)$ to attain a better estimate of Bob's variables. Then Eve can know an additional information carried by the variation of $\rho(X|a,e)$. Suppose Eve attacks Bob's information through a series of methods $E = \{E_{\rho_i}, \Pr(E_{\rho_i})\}$. Then after the QC the mutual information between Alice and Bob is $\xi_{\rho_0} I_{\rho_0}(A:B)$, where $\rho_0 = \coprod_{a,e} \sum_{E_{\rho_i}} \Pr(E_{\rho_i})\rho_i$. If Alice knew the $\rho_i$of each communication, the mutual information between her and Bob after the QC would become $\bar{I}_c(A:B) = \coprod_{a,e} \sum_{E_{\rho_i}} \Pr(E_{\rho_i})\xi_{\rho_i} I_{\rho_i}(A:B)$. Even though Eve cannot obtain as much information as $\bar{I}_c(A:B)$, she can utilize the knowledge of knowing Alice and Bob's channel better than Alice to learn certain additional information of no more than $\bar{I}_c(A:B) - \xi_{\rho_0} I_{\rho_0}(A:B)$-bit from one variable on average through the Markov chain $Eve \to Alice \to Bob$, where we have already supposed that H_0^5 and H_0^2 hypotheses are valid and all possible noises are just a perturbation to the ρ_0. Actually, even if only the noise type changed and $I(A:B)$ remains the same, the mutual information between Eve and Bob may be changed. Here, under the perturbation condition, this effect cannot help Eve to obtain the information more than $\bar{I}_c(A:B) - \xi_{\rho_0} I_{\rho_0}(A:B)$-bit. Although this additional information is obtained through the Markov correlation, the channel optimization is realized by the non-Markov way. Therefore, this additional information still belongs to the part of non-Markovian information, $I(E:B|A,\Phi_1,\ldots,\Phi_5)$. Actually the maximum non-Markovian information can be understood through another aspect. If Eve were ignorant the information carried by the variation of ρ_i, her estimate of Alice and Bob's channel would only be based on ρ_0. She can estimate this channel better just because she obtains certain additional information carried by the variation of ρ_i. Then the upper bound of the amount of non-Markovian information is given by $\delta I_\rho = \Theta(\coprod_{a,e} \sum P_{E_{\rho_i}} \rho_i) - \coprod_{a,e} \sum P_{E_{\rho_i}} \Theta(\rho_i)$, where δI_ρ describes the information transmitted by the variation of ρ_i. As previous discussion, we see that $I(\rho) \leq 2H'_{\sigma_0^2}$.

D. Mutual information estimate

While estimate Eve's maximum information attacked from Bob, Alice and Bob should estimate the mutual information between themselves precisely at first. For the Markov chain, $Eve \to Alice \to Bob$, if the mutual information between Alice and Bob is increased, the mutual information between Eve and Bob may be increased too. Then if Alice and Bob underestimate the mutual information between themselves, they may also underestimate that between Eve and Bob. Therefore, the accurate estimate of the mutual information is crucial to the security. Here, we only test the conditional noise and do not test the mutual information. Actually, from $I(A:B) = H(B) - H(B|A)$ we can see that if Alice's modulation is given, the mutual information can be tested through the conditional entropy estimate. It can be proven that if H_0^5 and H_0^2 hypotheses are accepted, the underestimated mutual information between Alice and Bob satisfies $\delta I(A:B) \leq -\delta H(B|A)$. The maximum $\delta H(B|A)$ can be given by the Eq. (5), and thus the maximum $\delta I(A:B)$ can be obtained. Also, while the H_0^5 and H_0^2 are accepted, the maximum under estimated mutual information between Eve and Bob satisfies $\delta I(E:B) \leq \delta I(A:B)$. Thus

$$\delta I(E:B) \leq -\delta H(B|A) \tag{7}$$

In the security analysis we always regard $I(A:B) - I(E:B)$ as the secret key rate. If Eve's information can not be obtained from the Markov channel, the underestimate of Alice and Bob's information do not affect the security. However, the underestimate is fatal here. During the reconciliation, some reconciliation information should be exchanged, the amount of which is determined by the estimated information. For example, if Alice and Bob want to construct m-bit common binary keys from one variable, then $m - I(A:B)$-bit information should be published. If the $I(A:B)$ is underestimated, then the $I(E:B)$ will be underestimated and more public information should be transmitted. Then the final amount of secret keys should be subtracted by $\delta I(E:B)$. Therefore, for the RRCVQKD the practical secret key rate should be given by

$$\Delta I_{prac} = I_{est}(A:B) - I_{est}(E:B) - \delta I(E:B), \tag{8}$$

where I_{est} describes the estimated information.

Eqs. (5) and (7) show the possible underestimate caused by the channel test. $\delta I(E:B) < \Delta I_{QC}$ will give a minimum accuracy for the normality test, where ΔI_{QC} denotes the theoretical secret key rate after the

QC. Actually, if we ignore the QC, the normality test is useless, since the maximum $\delta H(B|A)$ cannot exceed $H'_{\sigma_0^2}$. While we take the practical QC into account, the normality test becomes crucial. We can see that to guarantee $\delta I(E:B) < \Delta I_{QC}$ after the QC we should make $\xi_{\rho_0}|\delta I_{\rho_0}(A:B)| + \delta\xi_{\rho_0} I_{\rho_0}(A:B) < \Delta I_{QC}$, a sufficient condition of which is

$$|\delta H(B|A)| + \delta\xi_{\rho_0} I_{\rho_0}(A:B) < \Delta I_{QC}. \tag{9}$$

The ξ_{ρ_0} relies on the noise type and the QC. Then the normality test should guarantee Eq. (9) to be satisfied. Here we employ the χ^2, kurtosis and skewness tests to do the channel check, mainly because different QC sensitive with different errors. For example, in the QC of Ref. [10], they utilized the noise distribution while $|X| \gg 0$ to reduce the computational complexity, and consequently that efficiency is sensitive with the distribution at $|X| \gg 0$. Then the distribution estimate errors should be very small at $|X| \gg 0$. The χ^2 test only shows the summation of errors in all the intervals and thus is not proper for the estimate. The kurtosis and skewness tests are to check the high order moment and therefore have a good performance while we check the distribution at $X \to \infty$. Then kurtosis and skewness tests are effective for the QC presented in Ref. [10]. The accuracy requirement of the kurtosis and skewness test can be given by Eq. (9) and the concrete QC.

E. Summation

In the CVQKD, to ensure the probability of Eve's successful attack arbitrarily small, certain amount of secret keys should be discarded away to counteract the inaccuracy of the parameter estimate. Since the CVQKD is much sensitive with those parameters, the mount of discarded secret key may be exaggerated compared with the amount of secret keys. Therefore, while we consider the security, the statistical fluctuation of the estimate should be taken into account. The inaccuracies of the mean, variance and normality respectively require certain amount of secret keys to be compensated. An effective test should make all of Eqs. (4), (2) and (9) to be satisfied at first. Actually, it also should guarantee the total amount of compensated secret keys smaller than the theoretical amount of secret keys. The total amount of compensated secret keys can be given by

$$\begin{aligned}\delta I \approx \frac{S^2}{2N_0 \ln 2}[(t_{n-1,\alpha/2} + t_{n-1,\beta/2})^2/n \\ +(n-1)/\chi^2_{n-1,1-\beta} - 1] \\ +2(\chi^2_{K-4,\alpha} + \chi^2_{K-4,\beta})/n + \delta\xi_{\rho_0} I_{\rho_0}(A:B)\end{aligned} \tag{10}$$

Then the total amount of excess noise should be smaller than $\gamma G N_0$. Thus we approximately have

$$\begin{aligned}\frac{S^2}{N_0}[(t_{n-1,\alpha/2} + t_{n-1,\beta/2})^2/n + (n-1)/\chi^2_{n-1,1-\beta}] \\ +2\ln 2[2(\chi^2_{K-4,\alpha} + \chi^2_{K-4,\beta})/n \\ +\delta\xi_{\rho_0} I_{\rho_0}(A:B)] < \gamma G\end{aligned} \tag{11}$$

Here it can be seen that only when $S^2 < \gamma G N_0$, there exist a n that satisfies Eq. (11). Since G is always exponentially proportional to the minus of the length of the transmission line, the n should be exponentially proportional to the transmission distance.

V. CONCLUSION AND OUTLOOK

For the statistical fluctuation, parameters of an insecure system may show it secure topsy-turvy. Here, we solved it through the hypothesis test. During the test, we also estimated all the required unknown parameters. After discussing Eve's possible attacks, we showed the influence of the estimate inaccuracy to the security. It is showed that the error of the mean estimate introduces a equivalent noise to Alice and Bob's coding, the inaccuracy of the variance estimate cause certain amount of secret key to be discarded for the compensation and the inaccuracy of the normality test induce Alice and Bob underestimate their mutual information.

In conventional scenario, the underestimate of the mutual information between Alice and Bob may make the result more reliable, but here we show that in the RRCVQKD this underestimate can consequently induce the underestimate of the mutual information between Eve and Bob and thus may cause the insecurity on the contrary.

The statistical fluctuation is inevitable. To compensate it and obtain a reliable result, certain amount of secret keys should be sacrificed. We showed that to ensure the amount of sacrificed secret keys smaller than that of the distillable secret keys, an effective channel test should guarantee Eqs. (2), (4), (9) and (11) to be satisfied. Consequently we demonstrated that the minimum sample size will be exponentially proportional to the transmission length.

Finally, it can be seen that through this security verification, the security of the RRCVQKD and its reconciliation can be tested. While the reconciliation is neglected or its efficiency is always 100%, the normality test is useless, whereas if the efficiency of the reconciliation is sensitive with the noise distribution, the normality test is crucial.

Acknowledgement: Special thanks are given to Mr. X. N. Ji. This work was supported by the Science Foundation of China under Grant No. 60537020 and No. 60121503, and the Knowledge Innovation Project of the Chinese Academy of Sciences.

[1] C. H. Bennett and G. Brassard, In *Proceedings of IEEE International Conference on Computers, Systems and Processing, Bangalore, India, 1984* (New York: IEEE, 1984), pp. 175-179; IBM Tech. Discl. Bull. **28**, 3153-3163 (1985).

[2] Y. B. Zhao, Z. F. Han and G. C. Guo, Generalized Continuous Variable Quantum Key Distribution, arXiv: quant-ph/0604146, (2006).

[3] R. Namiki and T. Hirano, Practical limitation for continuous-variable quantum cryptography using coherent states, Phys. Rev. Lett. **92**, 117901 (2003).

[4] F. Grosshans and N. J. Cerf, Continuous variable quantum cryptography is secure against non-Gaussian attacks, Phys. Rev. Lett. **92**, 047905 (2004).

[5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph and P. K. Lam, Quantum cryptography without switching, Phys. Rev. Lett. **93**, 170504 (2004).

[6] F. Grosshans, G. Van. Assche, J. Wenger, R. Brourl, N. J. Cerf and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature, **421**, 238 (2003).

[7] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus and G. Leuchs, ContinuousVariable Quantum Cryptography: Beating the 3 dB Loss Limit. Phys. Rev. Lett. **89**, 167901 (2004).

[8] M. Heid and N. Lütkenhaus, Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction, Phys. Rev. A **73**, 052316 (2006).

[9] M. Heid and N. Lütkenhaus, arXiv: quant-ph/0608015, (2006).

[10] Y. B. Zhao, Z. F. Han, J. J. Chen, Y. Z Gui and G. C. Guo, arXiv: quant-ph/ 0603068, (2006).

[11] M. Legre, H. Zbinden and N. Gisin, arXiv: quant-ph/0511113 (2005).

[12] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri and P. Grangier, Phys. Rev. A **72**, 050303(R) (2005).

[13] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005)

[14] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[15] Y. B. Zhao, Y. Z. Gui, J. J. Chen, Z. F. Han, G. C. Guo, arXiv: quant-ph/0602019 (2006).

[16] S. S. Shapiro and M. B. Wilk, An analysis of variance test for normality (complete samples), Biomerika, 52, 591 (1965).

[17] E. J. Gumbel, On the rellability of the classical chi-square test, Anals of Mathematical Statistics, **14**, 253 (1943).

[18] S. M. Kendall and A. Stuart, The advanced theory of statistics, (1977).

[19] E. S. Pearson and H. O. Hartley, Biometrika tables for statisticians Vol. **2** (1972).

[20] E. S. Pearson, Note on tests for normality, Biomerika, 423 (1930).

[21] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui and G. C. Guo, Opt. Lett. **30**, 2632 (2005).

[22] G. Van. Assche, J. Cardinal and N. J. Cerf, Reconciliation of a quantum-distributed Gaussian key, IEEE Trans. Inform. Theory, **50**, 394 (2004).

[23] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. 27, 379 (1948).

[24] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer, Generalized privacy amplification. IEEE Trans. Inf. Theory, **41**, 1915 (1995).

[25] I. Bialynicki, J.Mycielski, Commun. Math. Phys. **44**, 129 (1975).

[26] The density function of the χ^2_n distribution can be given by $k_n(x) = \begin{cases} \frac{1}{\Gamma(n/2)2^{n/2}} \exp(-\frac{x}{2}) x^{(n-2)/2}, \text{ while } x > 0 \\ 0, \text{ while } x \leq 0 \end{cases}$.